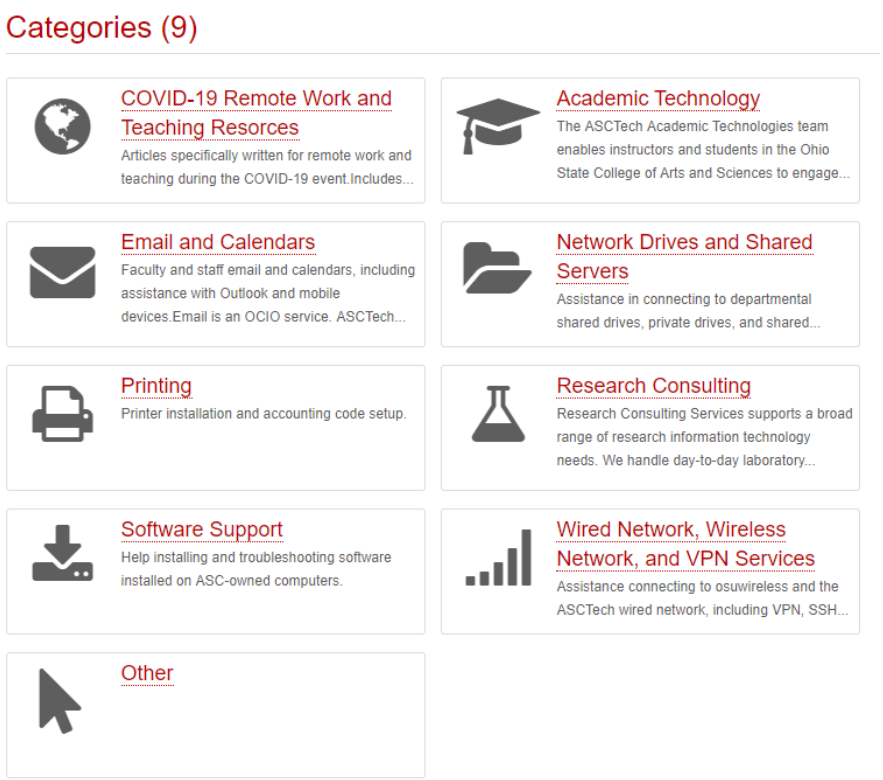
School of Earth Sciences ASC -IT Data Security Guidelines

Questions? Contact ASC-IT through the authorized channels of communication: **asctech@osu.edu**

ASC-IT professional for SES:
Brent Curtiss
Curtiss.3@osu.edu
Email for IT customer service asctech@osu.edu
125 South Oval Mall Rm 200F
(614) 688-3758
Data security, computers and computer service

Knowledge Base

https://osuasc.teamdynamix.com/TDClient/1929/Portal/KB/



Three and Green in 2018

https://osuasc.teamdynamix.com/TDClient/1929/Portal/KB/?CategoryID=6379

https://osuasc.teamdynamix.com/TDClient/1929/Portal/KB/ArticleDet?ID=29881

Three and Green in 2018 (TaG18) is a part of OCIO Enterprise Security's ongoing effort to enhance the university's computer security posture and better manage the risks associated with information technology. The tagline "Three and Green in 2018" comes from the goal of configuring every university IT device to score a high level of compliance or 'green' on the yearly Information Risk Survey (IRS), by 2018. The Three and Green initiative is university-wide, in all colleges and administrative units, and is backed by the Provost and the Board of Trustees. It is the university's explicit intent to provide a safer and more functional computing environment by reducing the risk of data loss, establishing better defenses against cyber-attackers, and complying with regulatory and legal requirements.

The *Information Security Control Requirements* (ISCR) provides a comprehensive set of security controls designed to meet these goals. ASCTech's mission is to implement the ISCR controls in the college while minimizing any resulting negative impacts on our research, instructional or administrative missions. Ultimately, ASCTech's goal is the same as always: Provide the college with a highly functional, secure and regulatory compliant computing environment utilizing the latest technologies. Three and Green is an important part of this overall effort.

The TaG18 requirements can be broken into six Information Security categories:

- Cataloging and Maintaining ASC's IT Asset Inventory.
- Classifying Stored Data Types and Securing Data Appropriately With Data Security Controls and Backups.
- Securing the College Network with Firewalls and Related Perimeter Controls.
- Minimizing the Attack Surface of College Endpoints with Patching, Anti-Malware, Encryption and Related Controls.
- Controlling Who is Authorized to Access Computing Devices and Institutional Data.
- Managing Application Development and the Purchasing of Information Technology Products.

How is this Accomplished?

What changes will be made to ASC owned devices?

Physical Asset Security

- Verify that every machine has an OSU Asset Tag. In partnership with unit administrative managers, comply with OSU asset procedures.
- Verify the primary user, location, manufacturer, and serial number are correct.
- Note the use type of the asset (Faculty/Staff, Grad Student, Student Lab, Research Lab, etc.).
- Note if the asset is considered a critical asset for Business Continuity / Disaster Recover.
- Ensure the asset is in the appropriate management console (Jamf Pro, SCCM, Red Hat Satellite.).
-

Data Security

- Match the data on the device to the OSU classification based on typical use and primary user input.
    - See attached OSU Data Classification document for explanation of Public, Internal, Private, and Restricted data. IT staff will also refer to these as S1, S2, S3, and S4 data, respectively.
    - OCIO Security's IDP Calculator can be helpful to gauge how to classify your data, and where you can store/use it.
- Ensure the device is bound to the ASC Active Directory (AD) and all login accounts are tied to the ASC AD.
- Primary user login account is unprivileged, and privileged accounts are separate and used only for privilege escalation.
- Ensure the device storage is encrypted.
- Ensure the device firewall is active.
- Install and verify anti-malware software (Symantec Endpoint Protection).
- Install and verify vulnerbility and patching reporting (Nessus).
- Provision a sensitive data scanner to aid in data classification and management, and provide safe harbor if the device is lost (Symantec DLP).
- Install data backup software (Code42, formerly called CrashPlan).

FAQ

Does this really lower OSU's risk?

Yes, each item of the TaG18 checklist is designed to reduce one or more facets of risk and is an accepted security practice.

Where can I find the OSU policies this initiative addresses?

OCIO Enterprise Security's "Cybersecurity for Ohio State"

https://cybersecurity.osu.edu/cybersecurity-ohio-state

In particular, the TaG18 actions are driven by the *Information Security Control Requirements* (ISCR).

Has ASCTech tested this configuration?

Yes, ASCTech staff have been running this configuration on our devices. In many cases, this software is already in use on faculty, staff, and devices around the college. The goal of TaG18 is to make sure *every* ASC owned device is configured to the ISCR.

Does ASCTech really have to see my laptop or home machine? Can I do it myself?

Yes, we also call this project Touch Every ASC Machine (TEAM) since certain items can only be done in person. Once all ASC devices have the TaG18 configuration, ongoing maintenance should be mostly automatic.

The project requires that ASCTech staff do the TaG18 items. Our checklist is attached for more granular reference of what we will be doing.

What if I choose to opt out of one or more of the University Three and Green in 18 requirements?

Any deviation from the TaG18 procedure will generate an exception. There are formal exception processes for requesting exemption from the various TaG18 controls.

Do I have to use ASC's backup software?

Yes. Faculty can only opt with with an exception signed off by the ASCTech Senior Director, initiated by unit ASCTech support. Our supported backup software, Code42 (formerly CrashPlan) has many features:

1. It is easy to use, and works with minimal user intervention. The Code42 product provides a continuous backup of new or changed data.
2. The data are stored remotely in a very secure local OSU facility that provides separation of originals and backup in the event of media failure, theft, or fire.
3. It backs up your computer no matter where you are. It can restore files from any location, as well. Backups are encrypted in transit.
4. It is approved for S4 data.
5. It allows multiple devices per user.
6. It has a large amount of storage, suitable for almost all endpoint devices.
7. It works on all desktop/laptop platforms we support.
8. Code42 backups are a key defense against ransomware threats. Local backups do not afford the same level of protection.

If you opt out, you risk data loss by not backing up your data, or risk data loss by having copies of data on removable storage. Depending on how you keep your backups, you may be violating OSU's Institutional Data Policy (IDP) or the Information Security Control Requirements (ISCR). By using Code42, you meet OSU requirements and ASCTech can assist you with the application.

Staff will not be permitted to opt out.

Are iOS and Android devices part of the TaG18 initiative?

ASC-owned iOS (iPhone, iPod Touch, and iPads) and Android devices are subject to TaG18.

What about my personal devices? Can I keep using them? How can I secure them?

For any non-ASC owned devices, you are responsible for following OSU's Institutional Data Policy (IDP). This may limit how you can use a personal device. For instance, data classified as restricted (S4) is not permitted on a personal device. All devices, personal or not, that hold OSU Institutional Data are subject to the ISCR.

ASCTech is happy to answer general questions and provide resources on securing personal devices. While we simply do not have the resources to provide extensive personal device support, we are here to help no matter what the device.

For general security guidelines applicable to personal machines, reference OCIO Enterprise Security's "Cybersecurity for You."

Software Purchase Consultation

https://osuasc.teamdynamix.com/TDClient/1929/Portal/Requests/ServiceDet?ID=13968

Service Description:

ASCTech provides consultation for software purchases from individual desktops to labs and classrooms. We'll find software that meets your needs, meets OSU's specifications, and is from an OSU-approved vendor.

Eligibility:

Available on all ASC-owned machines.

Standard Availability:

Service available 24/7; requests fulfilled during normal business hours. Please be aware that all software needing to be installed classrooms/labs needs to be brought to ASCTech's attention at least two weeks before the start of autumn semester. New software is only installed in classrooms/labs during the summer. Updates are installed over autumn, winter, and summer breaks.

What Is Included:

- Software purchasing consultation.
- Quote generation.
- Software installation.

Cost:

Consultation is free; cost of software depends on what is being purchased.

How to Get It:

Use the "Request Service" button, email asctech@osu.edu, or see phone/walkin information for the different support areas on the front page.